

FIG. 1 (PRIOR ART)

ELECTRONIC TRANSACTION SYSTEM

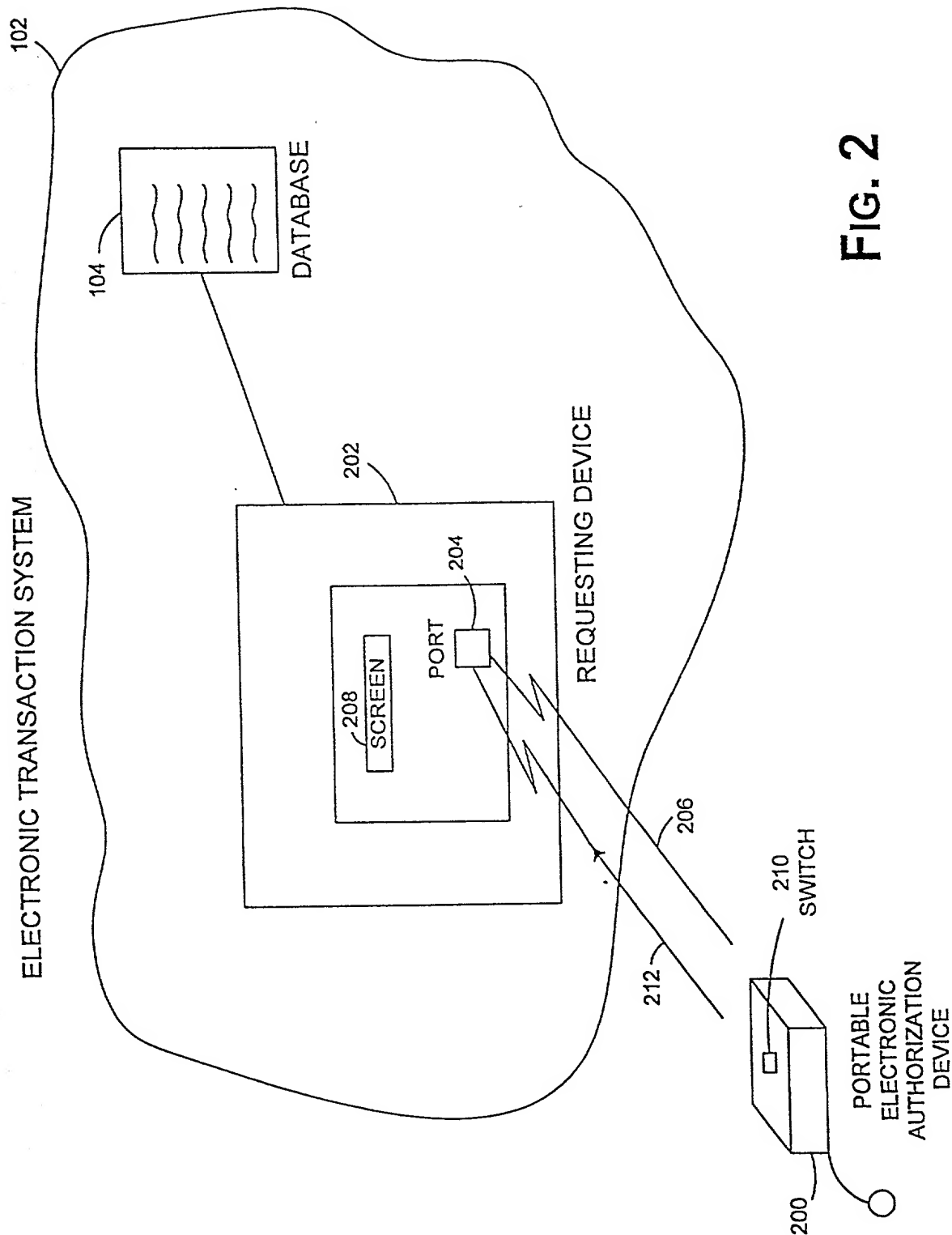


FIG. 2

PORTABLE ELECTRONIC AUTHORIZATION DEVICE

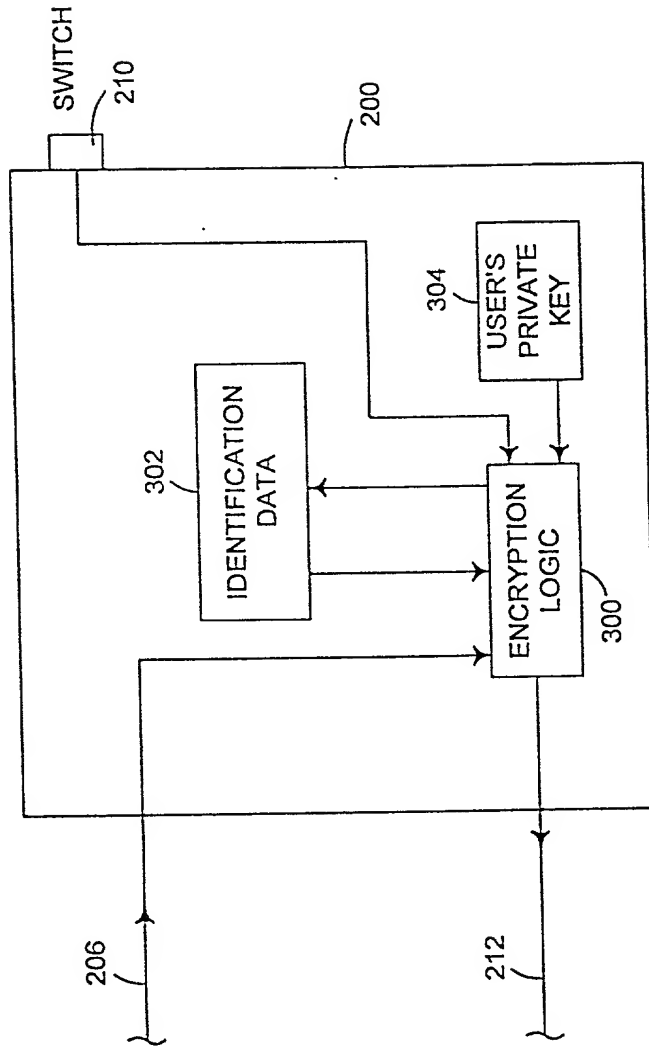


FIG. 3A

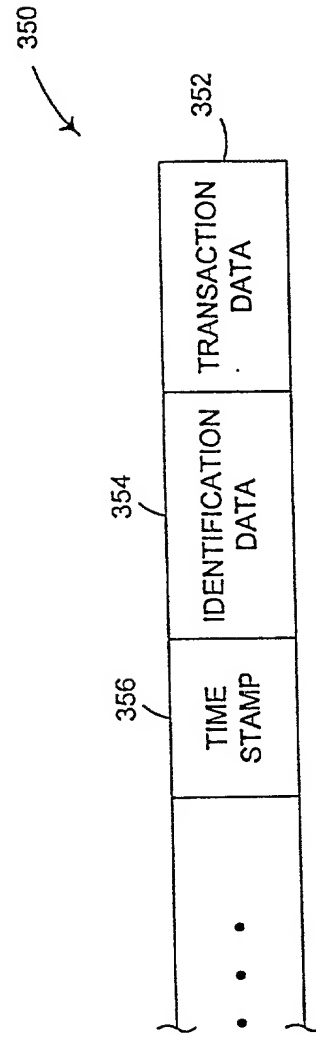


FIG. 3B

PORTABLE ELECTRONIC AUTHORIZATION DEVICE

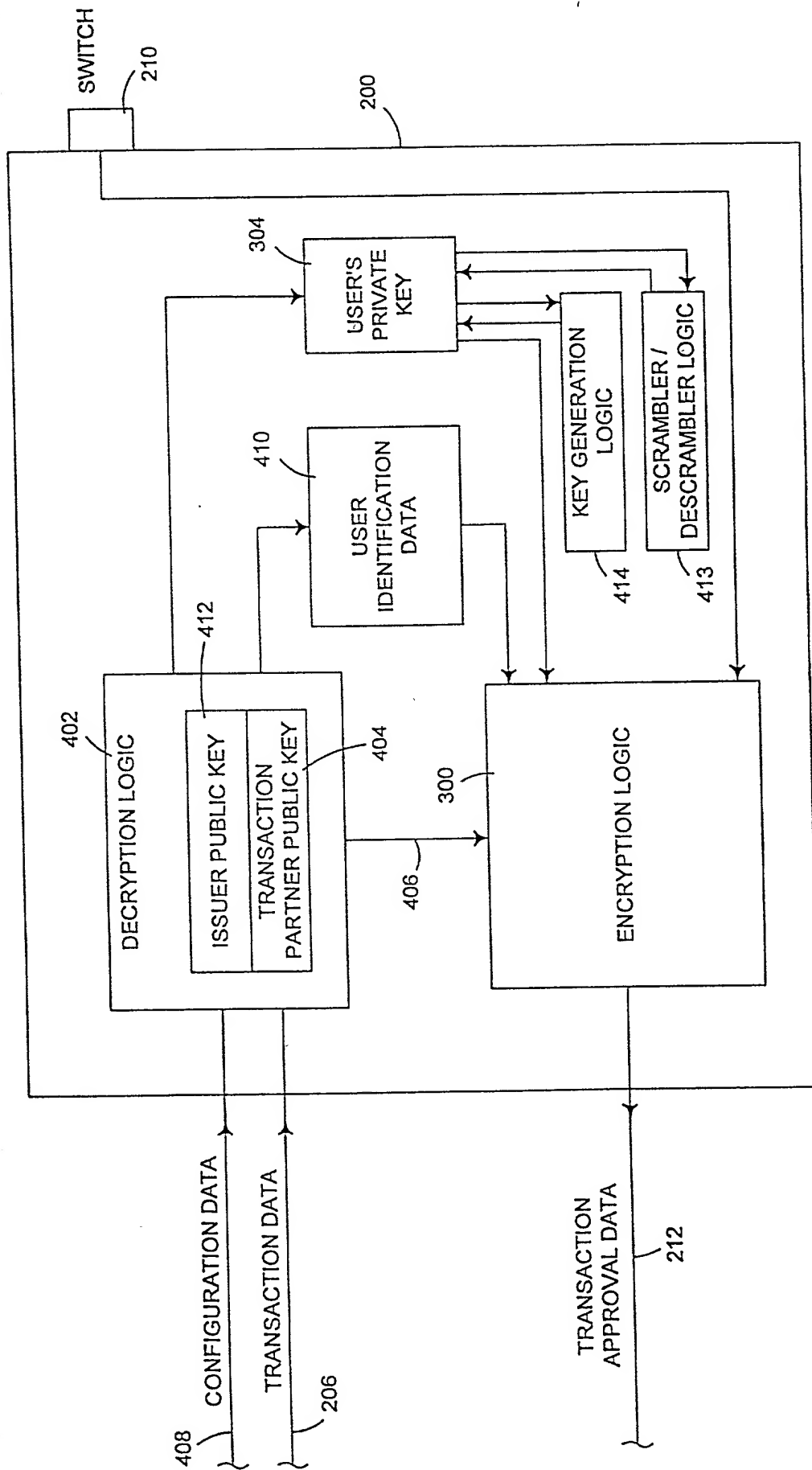


FIG. 4

PORTABLE ELECTRONIC AUTHORIZATION DEVICE

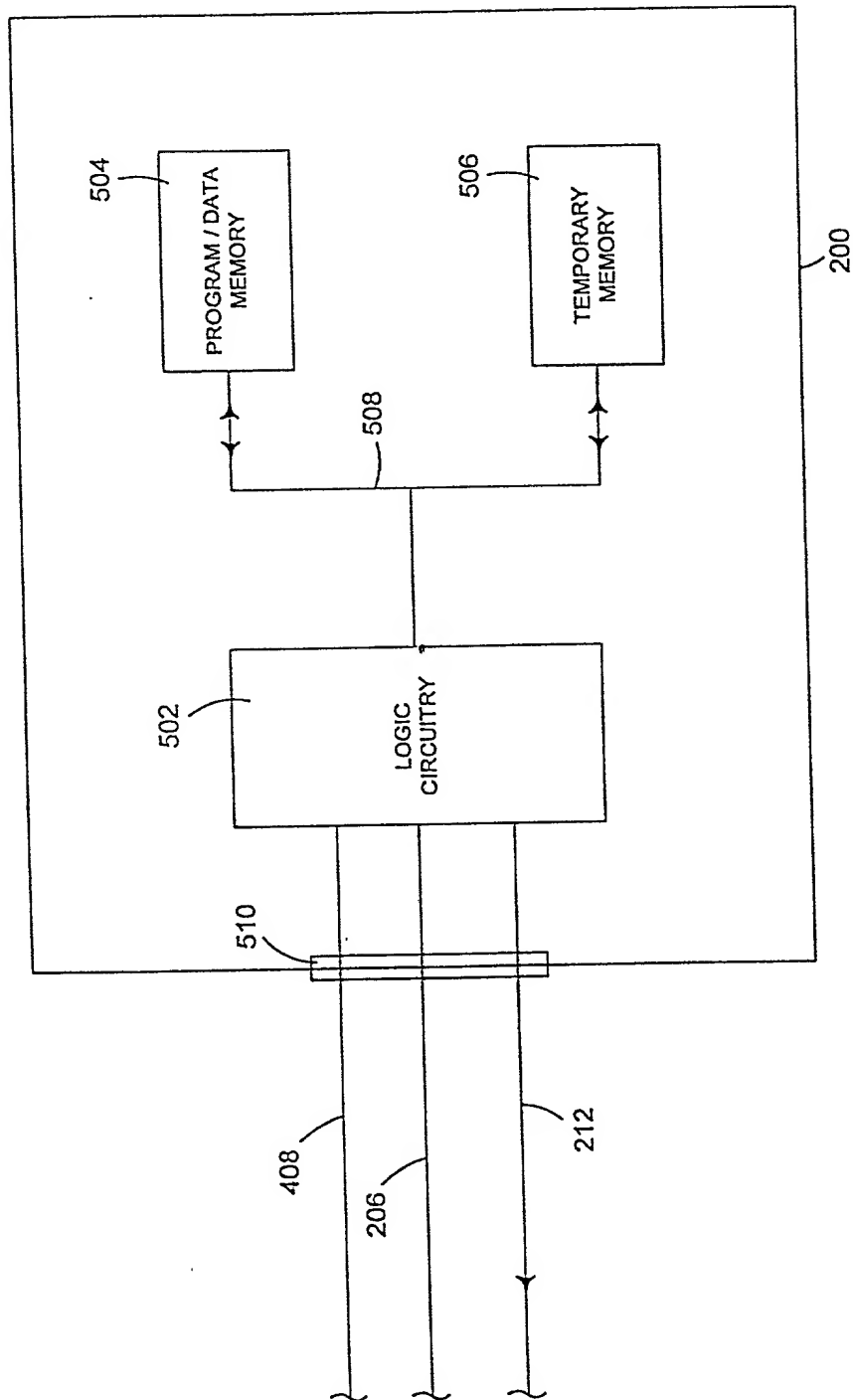


FIG. 5A

FIG. 5B

PORTABLE ELECTRONIC AUTORIZATION DEVICE

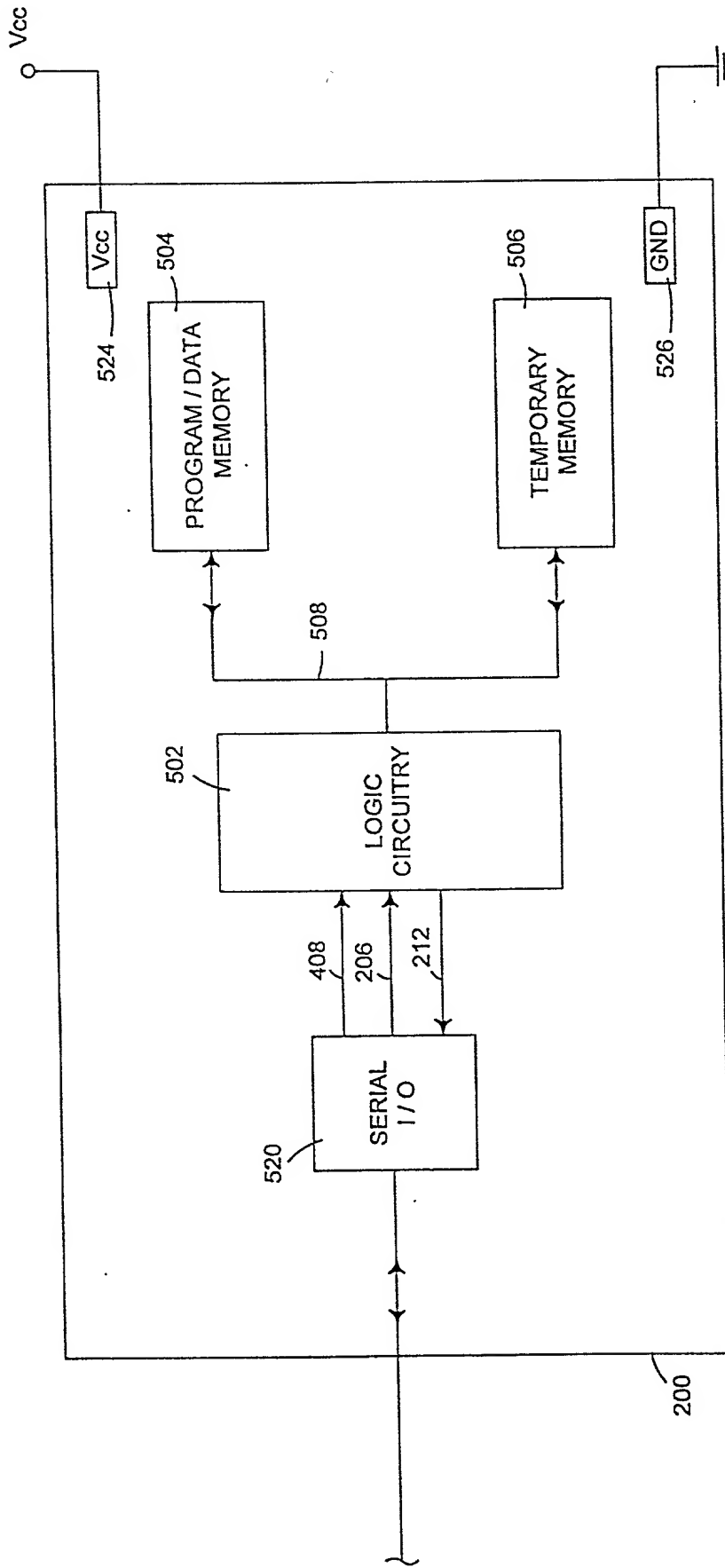


FIG. 5B

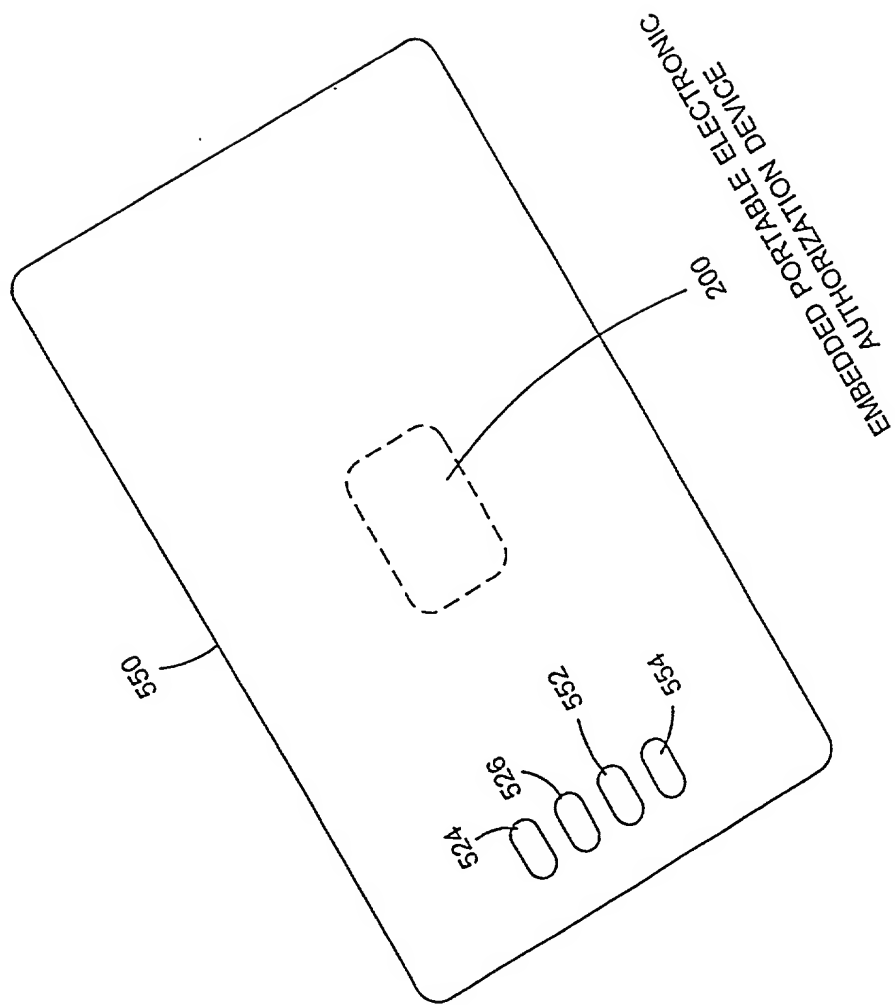


FIG. 5C

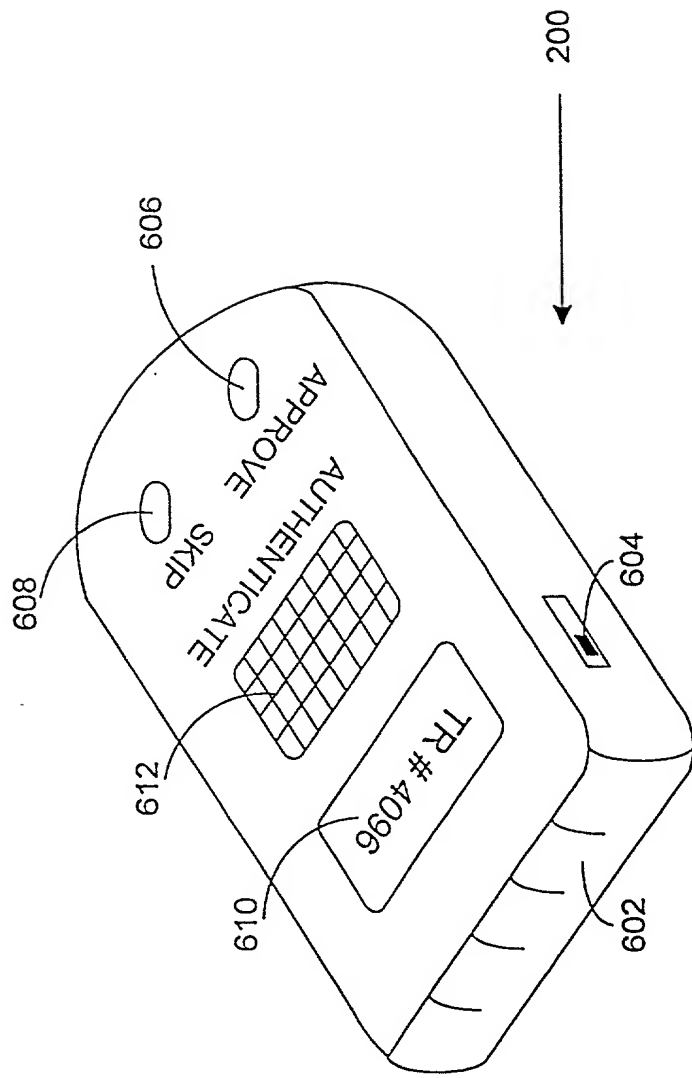


FIG. 6A

FIG. 6A

FIG. 6B

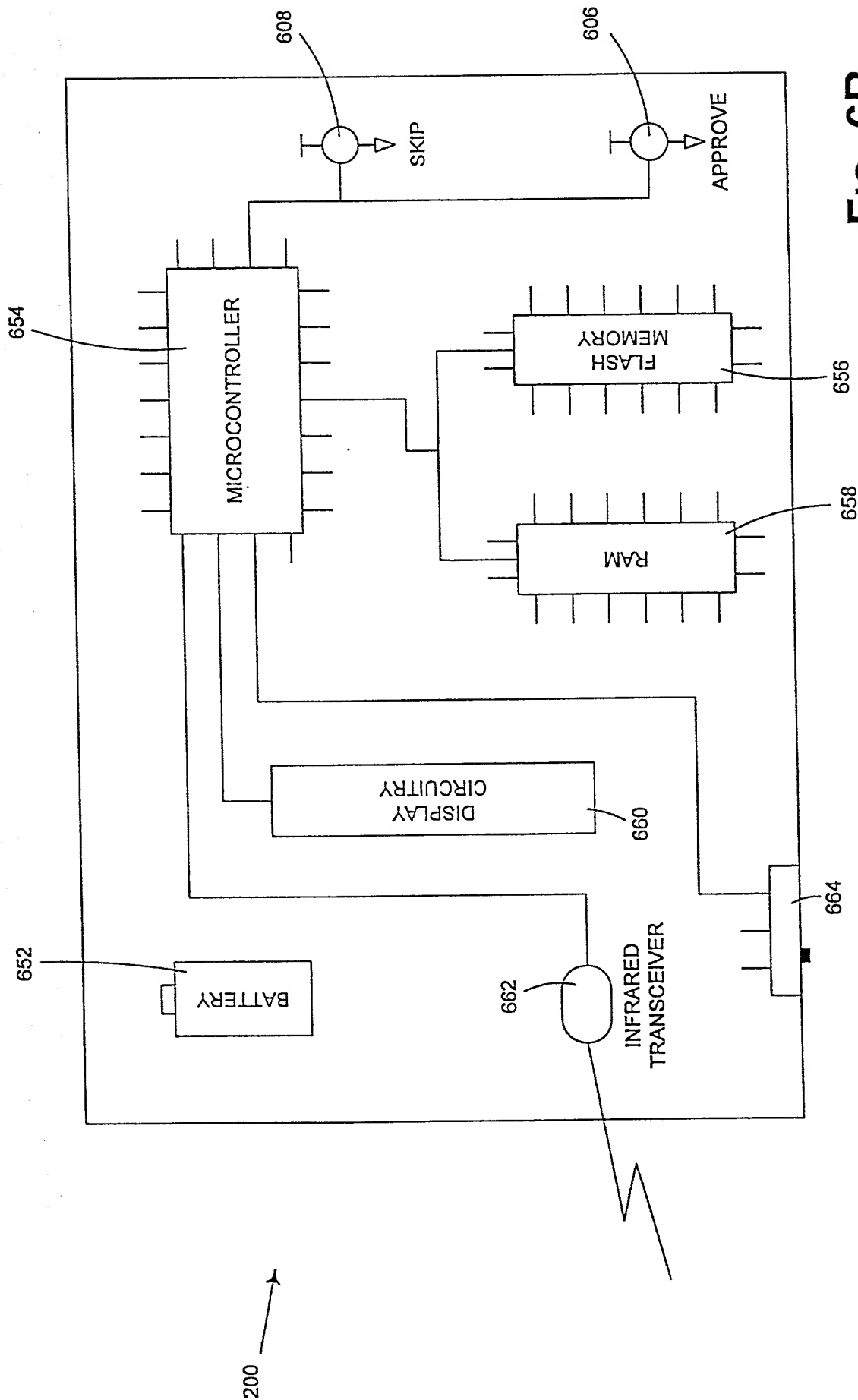


FIG. 6B

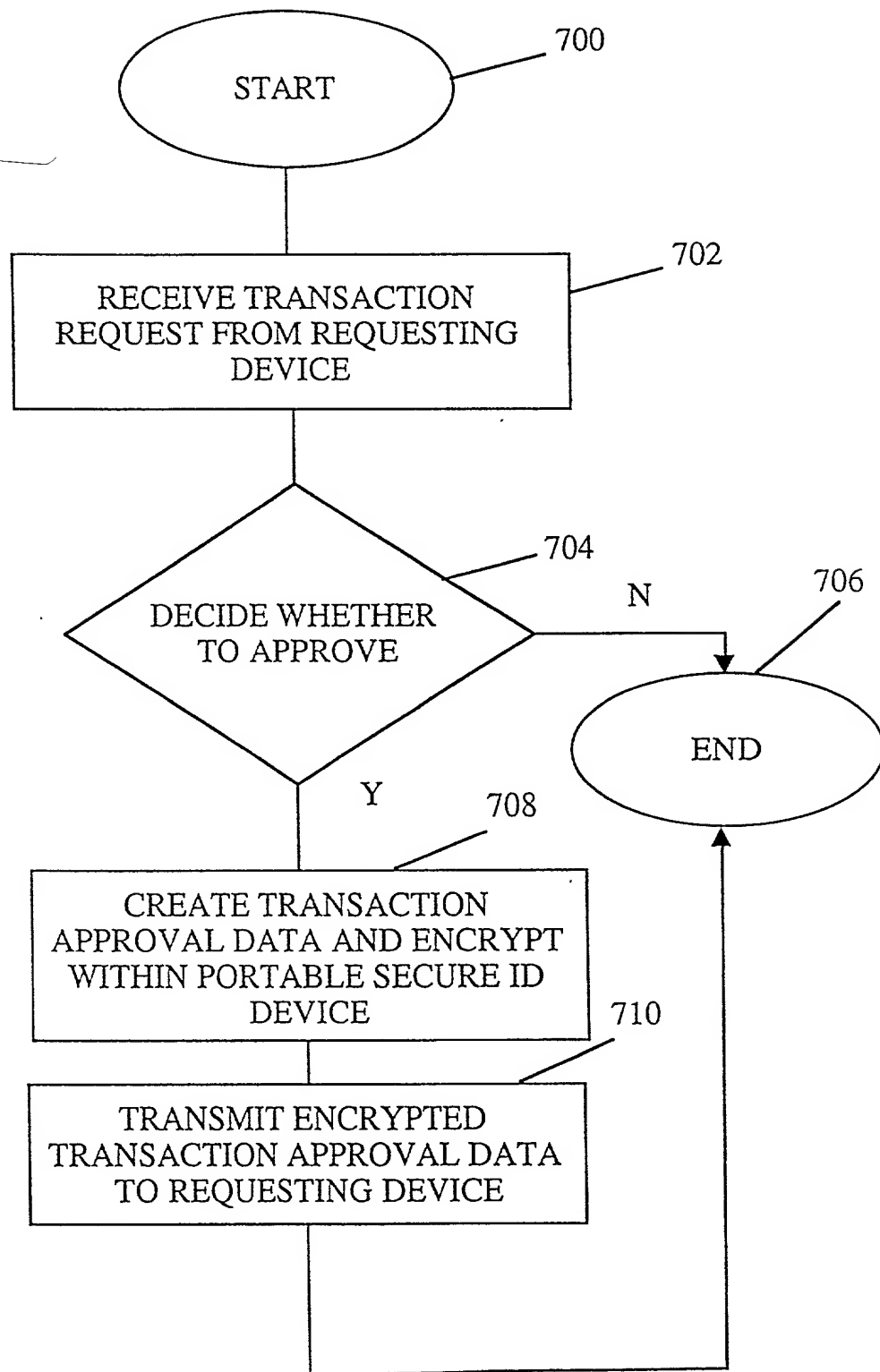


FIG. 7

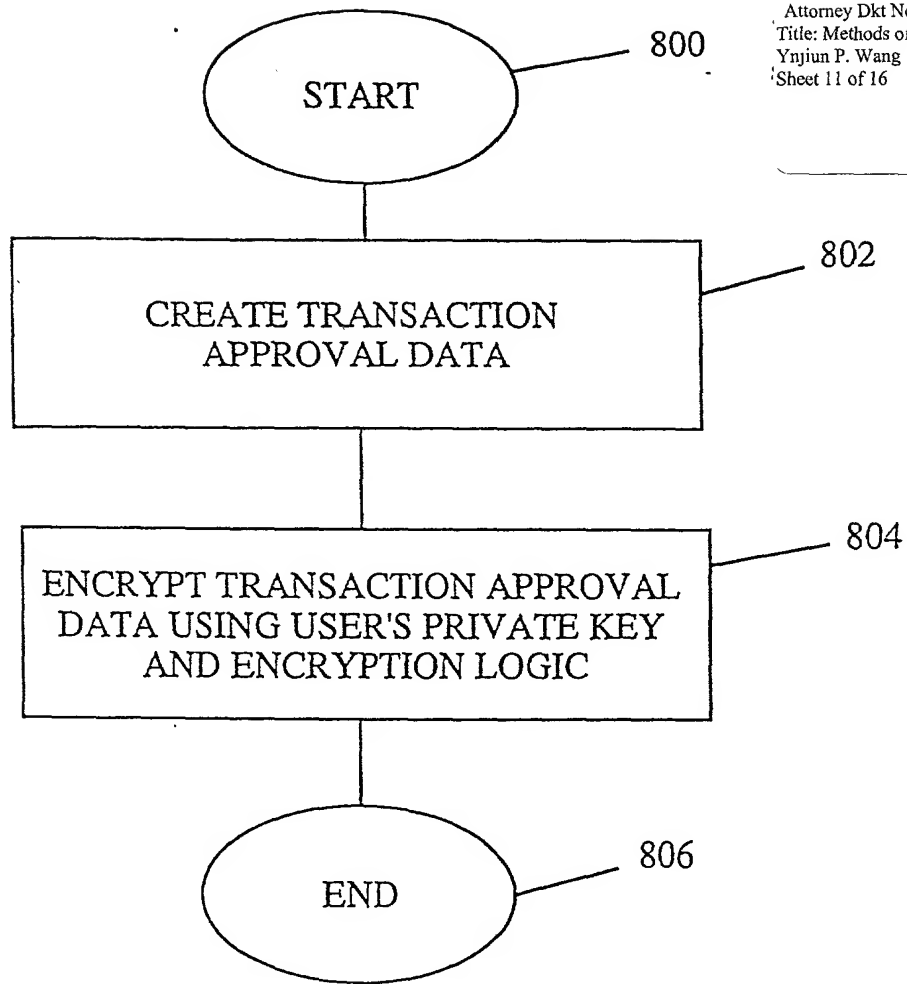


FIG. 8

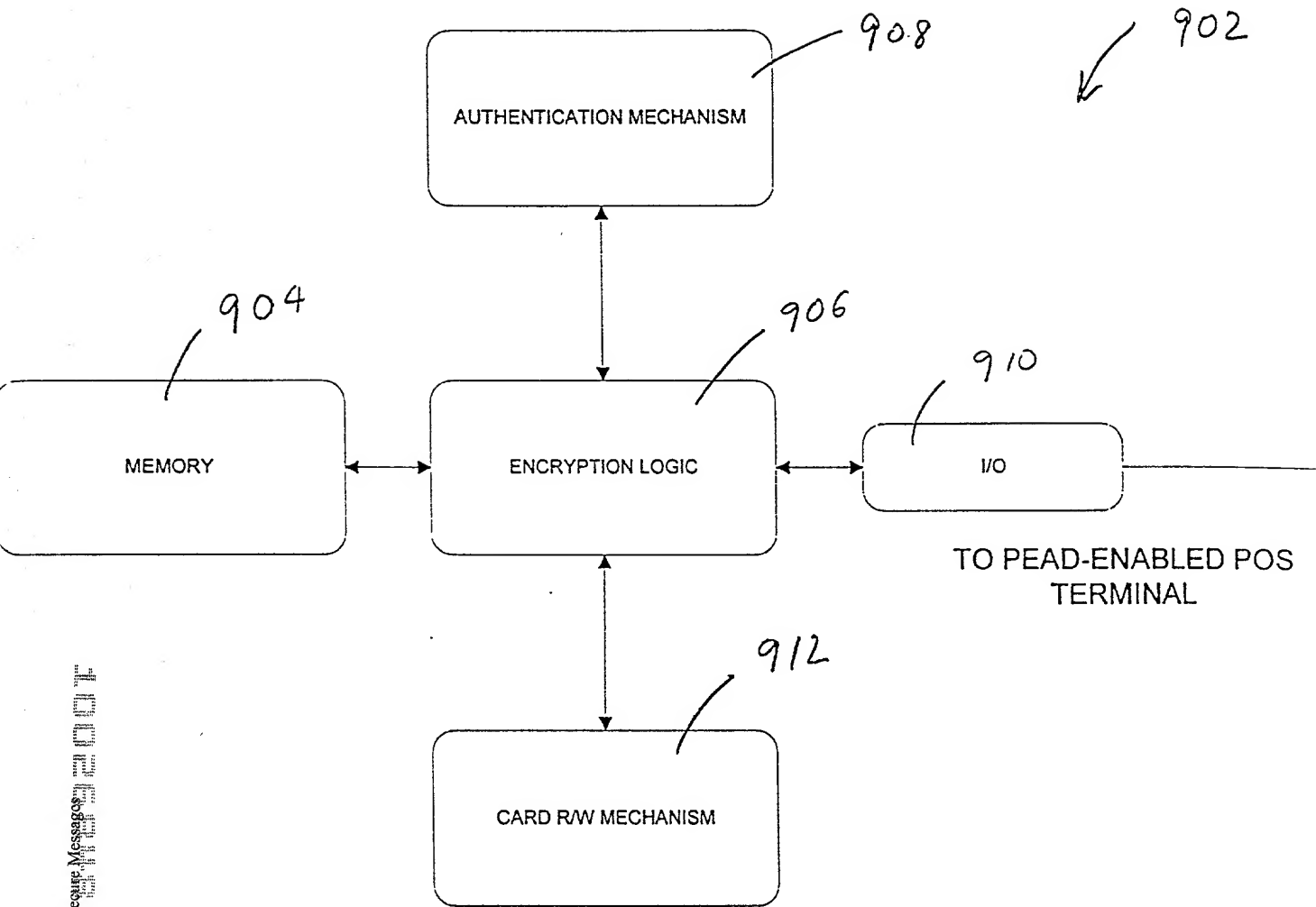


FIG. 9

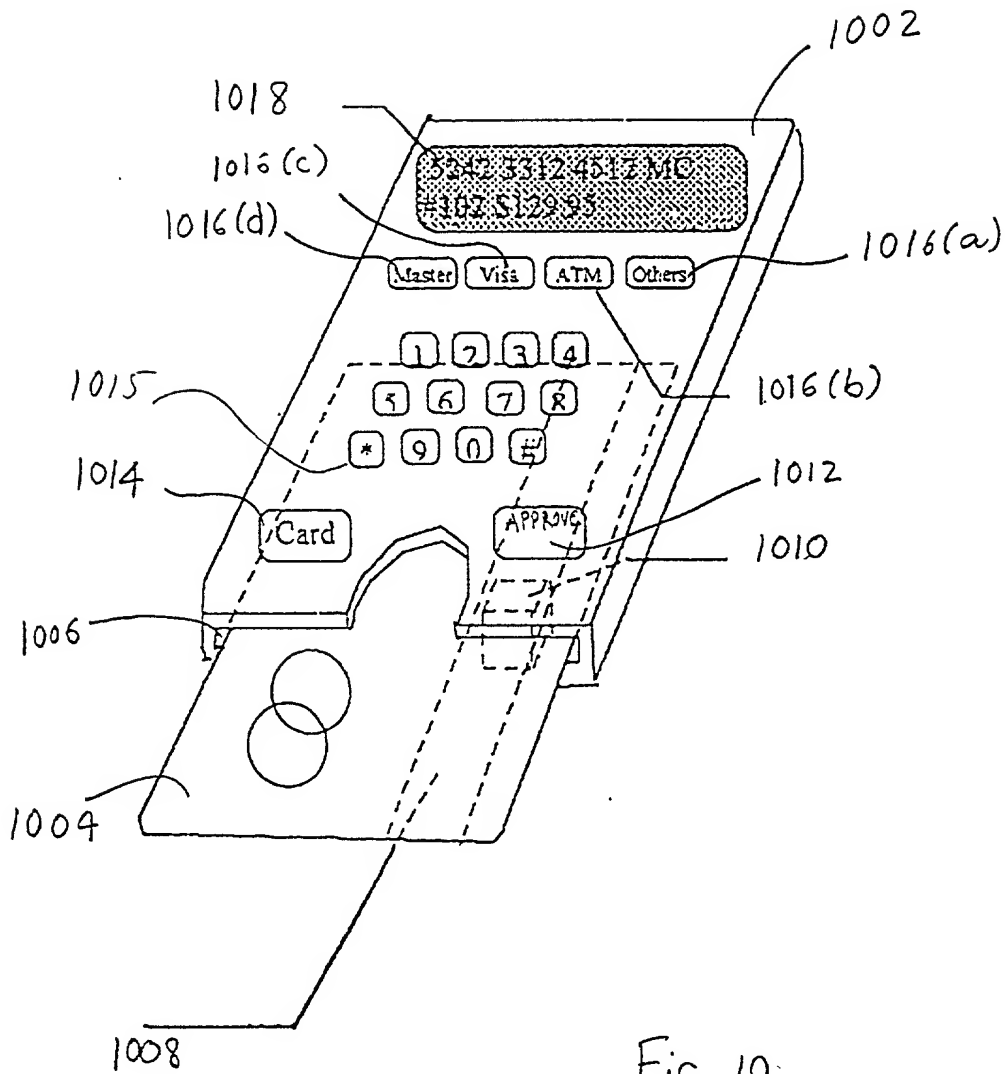


Fig. 10

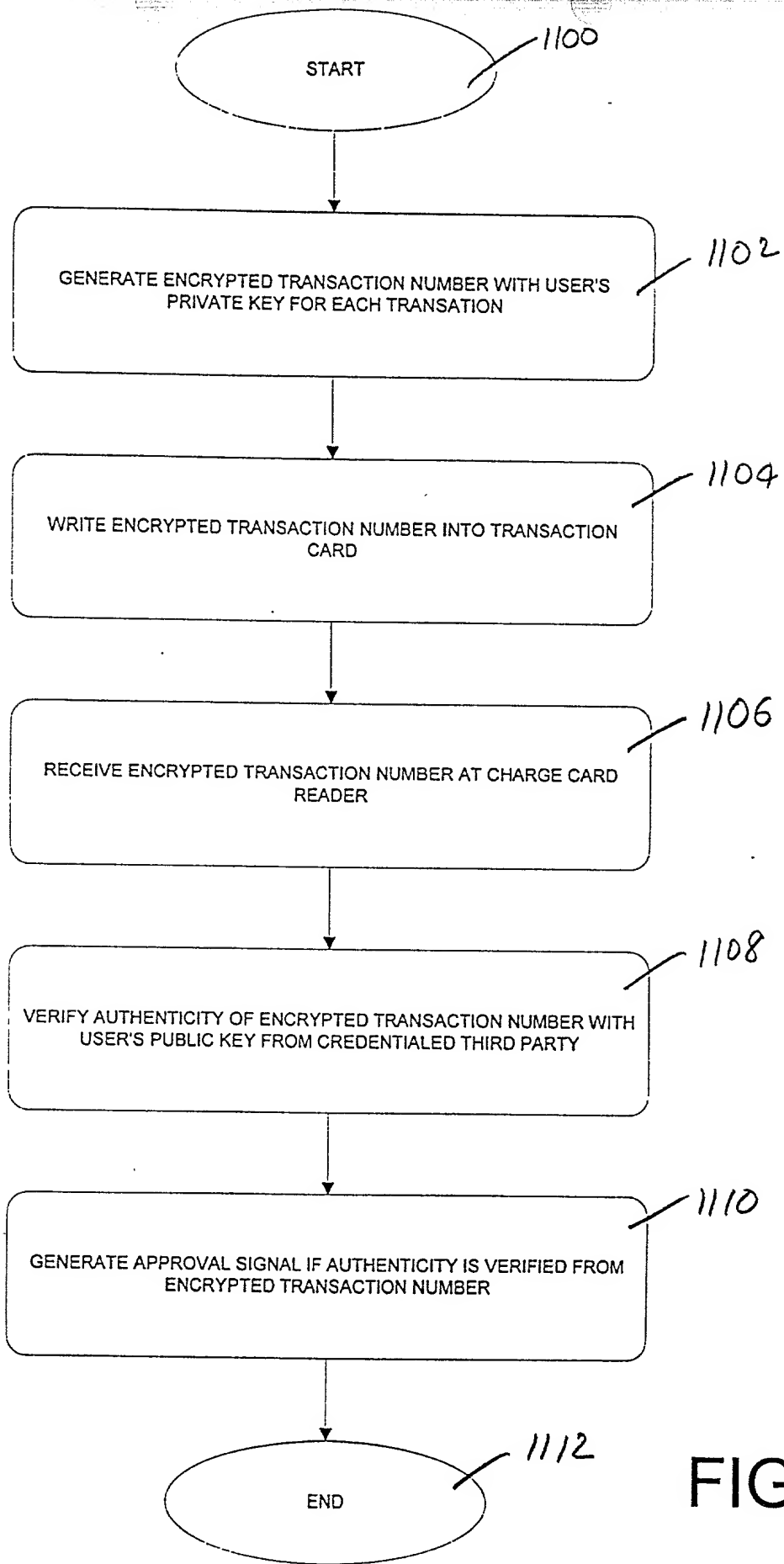


FIG. 11

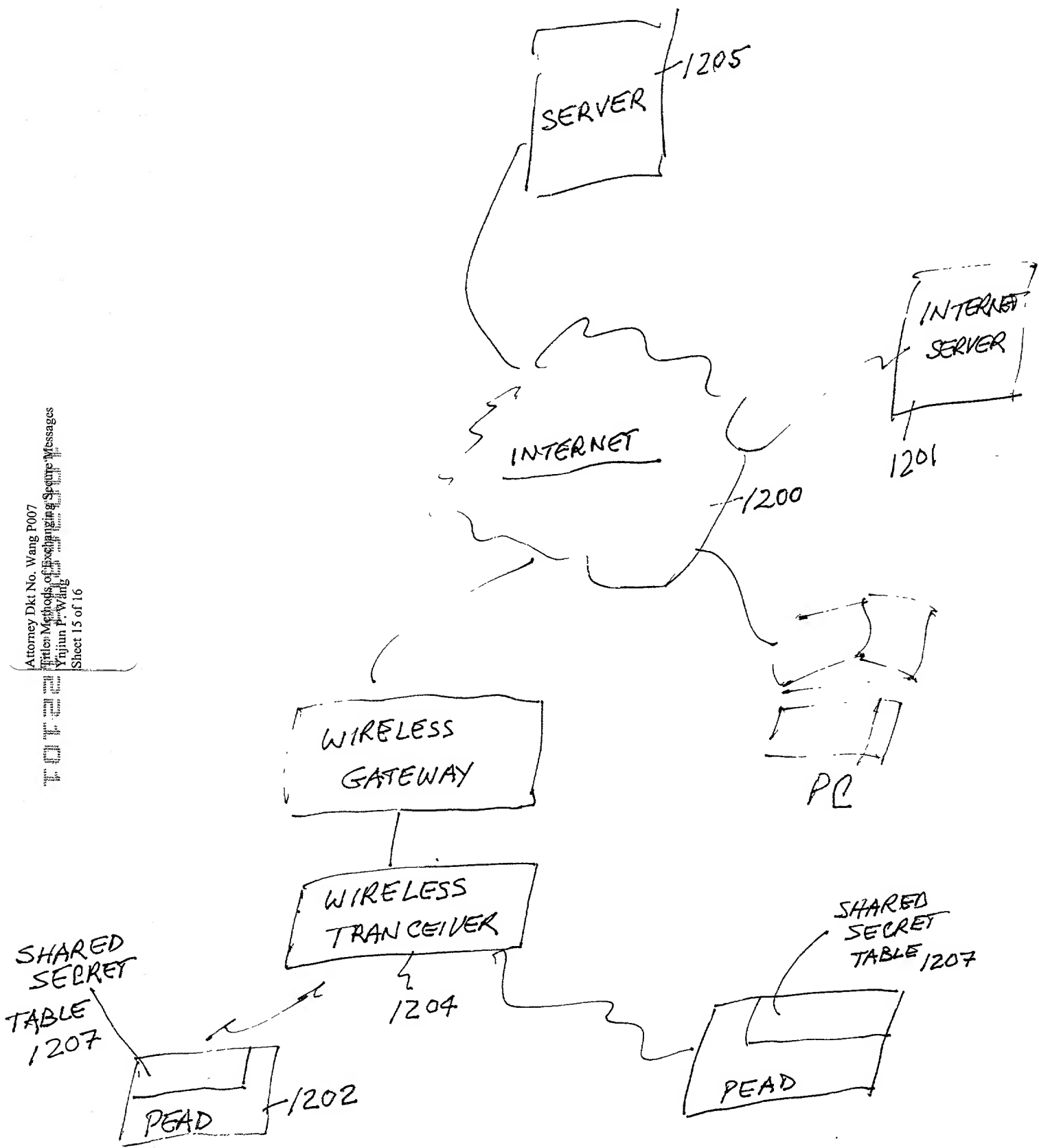


FIG 12A

Sender retrieves public key
information using receiver's i.d. - 1210

Sender derives shared secret
using receiver's public key - 1214

Sender encrypts message
with shared secret - 1216

Sender sends message
after appending receiver's i.d. - 1218

Receiver derives the
shared secret using sender's
user i.d. and sender's
public key - 1220

Store shared secret with
receiver's i.d. as an - 1222
index in receiver's PEAD

FIG 12B